AIR FORCE AND THE CYBERSPACE MISSION
DEFENDING THE AIR FORCE'S COMPUTER NETWORK
IN THE FUTURE

Shane P. Courville, Lt Col, USAF

December 2007

The Occasional paper series was established by the Center for Strategy and Technology as a forum for research on topics that reflect long-term strategic thinking about technology and its implications for U.S. national security. Copies of No. 63 in this series are available from the Center for Strategy and Technology, Air War College, 325 Chennault Circle, Maxwell AFB, AL 36112, or on the CSAT website at http://www.au.af.mil/au/awc/awcgate/awccsat.htm. The fax number is (334) 953-6158; phone (334) 953-6150.

Occasional Paper No. 63
Center for Strategy and Technology
Air War College

Air University
Maxwell Air Force Base, Alabama 36112

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Air Force and the Cyberspace Mission Defending the Air Force's Computer Network in the Future	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Center for Strategy and Technology,Air War College,Air Univeristy,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

A little over year ago, in November 2005, the Secretary of the Air Force Michael W. Wynne and Air Force Chief of Staff General T. Michael Moseley wrote a joint letter to all airmen of the Air Force, which defined a new mission statement which included the concept of cyberspace. Cyberspace was defined as including network security, data transmission and the sharing of information. Although the Air Force and the Department of Defense (DOD) in general, have numerous safeguards in effect to protect systems and their networks, DOD relies on a system that is passive when encountering cyber threats. This paper recommends the Air Force pursue research in quantum encryption and security, and continue to examine computer security techniques for the mid-term and beyond. The Air Force should continue future planning efforts to anticipate and develop countermeasures to emerging threats in order to proactively protect and dominate the cyberspace domain of the future.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**58**	

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

List of Illustrations

Page

Abstract

A little over year ago, in November 2005, the Secretary of the Air Force Michael W. Wynne and Air Force Chief of Staff General T. Michael Moseley wrote a joint letter to all airmen of the Air Force, which defined a new mission statement which included the concept of cyberspace. Cyberspace was defined as including network security, data transmission and the sharing of information.

Although the Air Force and the Department of Defense (DOD) in general, have numerous safeguards in effect to protect systems and their networks, DOD relies on a system that is *passive* when encountering cyber threats. This paper recommends the Air Force pursue research in quantum encryption and security, and continue to examine computer security techniques for the mid-term and beyond. The Air Force should continue future planning efforts to anticipate and develop countermeasures to emerging threats in order to proactively protect and dominate the cyberspace domain of the *future*.

Chapter 1
Introduction

*I see the mission of the Air Force as: Deliver sovereign options for the defense of the United States of America, and its global interests – in air, space, and **cyberspace**.*

— Honorable Michael W. Wynne, Secretary of the Air Force[1]

The United States Air Force was the first of the military services to include cyberspace in its mission statement. The Secretary of the Air Force and the Air Force Chief Staff, shortly after announcing the new mission statement released a joint Letter to Airmen on 7 Dec 05, wherein Secretary Wynne stated "we have quite a few of our Airmen dedicated to cyberspace….from security awareness, making sure the networks can't be penetrated, as well as figuring out countermeasures. The Air Force is a natural leader in the cyber world and we thought it would be best to recognize that talent."[2] In the same news release, the Air Force gave a more defined view of cyberspace: "the term cyberspace includes network security, data transmission and the sharing of information."[3] Finally, the joint Letter to Airmen points out: "As Airmen, it is our calling to dominate Air, Space, and Cyberspace."[4] The way Airmen will meet the direction Air Force leadership advocates, particularly in cyberspace, rests on a clear understanding of exactly what that calling entails.

Cyberspace is not a very new concept. The term cyberspace[5] was first used in the 1982 science fiction novel *Burning Chrome*, by William F. Gibson. It was later popularized in Gibson's next novel, *Neuromancer*. While popularized, it remained an elusive term to define. Nearly twenty years later, President Bush, in 2003 set forth a policy to *secure cyberspace* in his National Strategy to Secure Cyberspace.[6] Soon thereafter, the 2004 National Military Strategy included the domain as an operational battlespace requirement.[7] Yet, cyberspace is not a term found in printed dictionaries, and on-line sources have widely varying definitions. In fact, once the Air Force claimed the virtual high ground called cyberspace last year, a flurry of activity quickly began to define exactly what it claimed.

To that end, the Air Force stood up a Cyberspace Task Force in January 2006, led by Dr. Lani Kass,[8] chartered to investigate cyberspace as a domain in and through which the Air Force flies and fights. Following her appointment, Dr. Kass defined the initial goal of the task force as developing a set of recommendations that included designing a strategy for dominance across domains, evolving operational concepts for cyberspace and changing doctrine for the mission.[9] One of the first items the task force tackled was to come up with a common definition of cyberspace, which Dr. Kass admits was a struggle as the team poured through hundreds of opinions during their research. The task force defined cyberspace as a warfighting domain bounded

by the electromagnetic spectrum or the "maneuver space of the electromagnetic spectrum."[10] Surely, sister services in DOD may have other ideas on defining cyberspace. However, at this time a full and complete definition is not possible, as cyberspace is an immature science and a full understanding of the domain is years away. Therefore, any definition of cyberspace must remain flexible and adaptable in order to allow future innovations to take its course.

This paper argues that America's future adversaries *can, and will* use information technology as a means to wage warfare in the cyberspace domain against the United States. The Air Force is highly dependent on computers and information operations, and will be even more dependent in the next twenty years. The majority of computers, their operating systems and software purchased by the Air Force are commercial off-the-shelf (COTS) components, often manufactured abroad due to cheaper cost. Thus, foreign countries could place hidden components inside the computers, making the computers vulnerable for attack and/or spying. This paper succinctly illustrates how this presents significant vulnerabilities to the Air Force's cyber domain. Furthermore, Air Force networks are connected to and utilize the internet, which is also vulnerable for exploitation. These threats are real and are succinctly summarized in a crystal clear 2003 information security report: "The U.S. Department of Defense (DOD) relies too much on commercial software, doesn't know who is creating the software, and faces other significant cybersecurity problems."[11]

This paper explores the topic of defense of the cyberspace domain by the Air Force, with a focus towards future vulnerabilities and actions underway to protect the domain. It provides a brief background of the Air Force's reliance on standard computer configurations, operating systems, software, and network connectivity. It then reviews the vulnerability of computer systems, processes in place to protect the Air Force network, and looks at the future towards 2030 to find potential threat vulnerabilities. This paper's look at defending cyberspace provides several recommendations this author advocates as a defense to mitigate against potential adversaries.

Chapter 2
Know Thy Enemy – He May Be Armed With Bits and Bytes

"Major Cyberspace Vulnerabilities Will Be Used Against Us."
—Richard A. Clarke, Testimony to Congress[12]

Richard A. Clarke's [13] testimony to a Congressional Committee in 2003 emphasized today's growing threat. He began his testimony discussing the cyberspace threat and vulnerabilities, stating:

> For many, the cyber threat is hard to understand. They think that these cyber attacks are unfortunate, but are just a cost of doing business, just a minor nuisance in a multi-trillion dollar economy. No one has died in a cyber attack, after all, there has never been a smoking ruin for cameras to see. Such reasoning is dangerous. Implicit in such thinking is the unarticulated notion that the only cyber attacks that can happen in the future are those similar to what has happened in the past. Implicit is the 20th century notion that if it is not a smoldering heap with a body count, there has been no real damage…the threat is really very easy to understand…if there are major vulnerabilities in the digital networks that make our country run, then someday, somebody will exploit them in a major way doing great damage…meanwhile, short of the Big Attack, there is damage being done every day…the culprits range from cyber joy riders, to thieves, to organized criminals, to corporate spies, to terrorist groups, to nation states.[14]

Data available succinctly supports Mr. Clarke's claims. Research readily shows numerous reports of cyber attacks to various computers, operating systems, software applications. One such organization, the SANS Institute[15], working with the FBI's National Infrastructure Protection Center, provides information on likely targets an enemy may attack. The SANS Institute provides an annual report of the Top Twenty Internet Security Attack Targets which depict the most vulnerable computer systems and software. The top five on the target list of vulnerable operating systems in 2006 all belonged to Microsoft, including its Internet Explorer and Microsoft Office applications.[16] The announcement of the vulnerability list, detailing those specific software programs is disturbing. The Air Force announced in early 2006 that it

committed to a five-year, $50 million contract with Microsoft to place a Standard Desktop Configuration (SDC) in its computers.

The word "Microsoft" [17] has become synonymous with computers, to include the Air Force's own computer systems. Essentially, *Microsoft is everywhere* – ask anyone today in the computer industry what "Word, Excel or PowerPoint" is, and the likely response will point toward software the company produces and installs in computer systems. Microsoft's "corner of the market" brings both good and bad. Microsoft offered a rare glimpse of the extent of infected Windows systems at a June 2006 technical conference, reporting a significant percentage of the world's computers have been infected by keystroke loggers, Internet Relay Chat bots[18] and rootkits[19]. Microsoft security researchers used data collected from its Malicious Software Removal Tool (MSRT) to produce a clear picture of the malicious software (also called malware)[20] against Windows. Microsoft has removed at least 16 million instances of malware from 5.7 million Windows-based computers since the first iteration of the Removal Tool in January 2005. That equates to one virus, Trojan[21], rootkit or worm every 311 times it scanned one of the 270 million computers running on Microsoft's Removal Tool. The Tool removed at least one Trojan from about 3.5 million unique computers; of the 5.7 million infected Windows machines, about 62 percent were found with a Trojan or bot.[22]

Microsoft's confirmation of the widespread problem is consistently highlighted in numerous periodicals warning institutions and organizations of the issue. Consider an example described in a recent article in SecurityFocus[23], an online source of internet and computer security information.

> On December 1, 2005, two e-mail messages were sent from a computer in Western Australia to members of two different human rights organizations. Each e-mail message carried a Microsoft Word document with a previously unknown exploit that would take control of the targeted person's computer and open up a beachhead into the group's network. The attack failed, as did a second attempt to infiltrate the same human-rights group a week later, due in no small part to an overabundance of caution on the part of the e-mail security provider MessageLabs, which initially blocked the emails based on the strangeness of the Word attachments. The attacks only targeted a single person at each organization and, after the two attempts, never repeated.[24]

The significance of this event was that it was a *low-volume attack* – aimed at only two computers. These low-volume attacks are rapidly becoming a major issue for the anti-virus and computer-security industries. Defense mechanisms, past and present, are geared to counter *high-volume Trojans*, which are at the top of deterrence lists, since they could affect a larger number of people. The impact, however, of *either* type of attack can cause the same devastating effect.[25] Trojans, in the case just described, only targeted a single person at two different organizations via an email message that carried a Microsoft Word document containing a previously unknown exploit. The majority of Trojan programs, almost 70 percent, use a malicious Word document as the vehicle for the attack. So far, hackers have been able to stay ahead of the security patches developed to tighten the loopholes in Word. Hackers are also becoming more creative by changing their method of attack, as a recent analysis showed PowerPoint and Excel documents are becoming the medium of choice.[26] However, Microsoft continues to focus on countering known security vulnerabilities in its software systems. This cat and mouse game continues daily throughout the world.

The United States Computer Emergency Readiness Team was established in 2003 to protect the nation's internet infrastructure and coordinate defense against and responses to cyber attacks across the nation. Part of the Department of Homeland Security, it interacts with federal agencies, state and local governments, industry professionals, and others to improve information sharing and incident response coordination and to reduce cyber threats and vulnerabilities.[27] The latest data from the Team indicates that 84 percent of computer attacks are phishing, a criminal activity wherein the violator attempts to gain passwords or items such as credit card details. In the Microsoft Word cases previously illustrated, Trojans only comprise about three percent of the cases, and therefore are not the primary the focus today, which may be why the Team did not issue any warnings or threat advisories regarding the attempts.

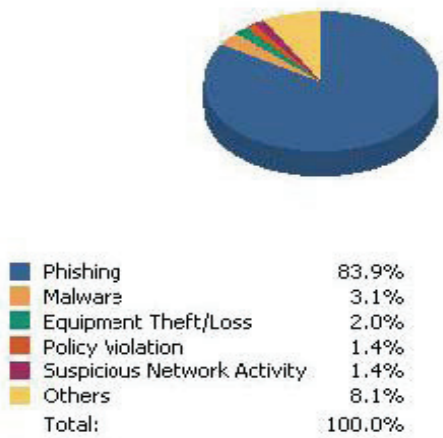

Figure 1: Top Five Computer Incidents and Events, 4th Quarter, FY 2006[28]

This low volume of Trojan attacks may account for the reason the Team did not issue a warning to users. Perhaps another reason could be the Team assumed most Americans are protecting their own computers with anti-virus software.

The Air Force Computer Emergency Response Team (AFCERT) acts as the single point contact for monitoring and reporting network security intrusion attempts. AFCERT works alongside all major command network operations and security centers and base-level network control centers. The team integrates their efforts to ward off intruding attempts by hackers and as well as viruses. Additionally, the group works with the Air Force's Information Warfare Center to help develop countermeasures against emerging threats, using an arsenal of both hardware and software, all in an effort to defend the entire computer system. The Air Force's experts also work with commercial anti-virus software developers, exchanging information in order to improve technology against the myriad of emerging computer threats. The exchange works both ways, as commercial industry experts are critical for the Air Force's cyber defense plan as well. One of the most recent examples occurred in August 2006, when the Air Force selected a popular anti-virus manufacturer, McAfee, as a tool help prevent intrusions to its network.[29] McAfee's software will also add a layer of defense against spyware, malware, worms and other vulnerabilities to Air Force computers.

The good news for most US computer users, including the Air Force, is the majority of computers utilizes some form of protection software – often free or provided with the computer when it is purchased. Anti-virus software can, for example, *passively* defend the computer against malware. However, this may mislead a user to assume his computer is protected, when in reality, the computer is wide open for exploitation.

Data from the government's Computer Emergency Readiness Team's partner, the Computer Emergency Response Team Coordination Center (CERT/CC)[30] reveals the tip of what may be considered a significant vulnerability of computer systems. Vulnerability incidents have increased from only a few hundred per year in the 1990s to 5,990 reports in 2005. The Air Force faces the same attacks and vulnerabilities since the service uses the identical hardware and software programs available in the commercial market.

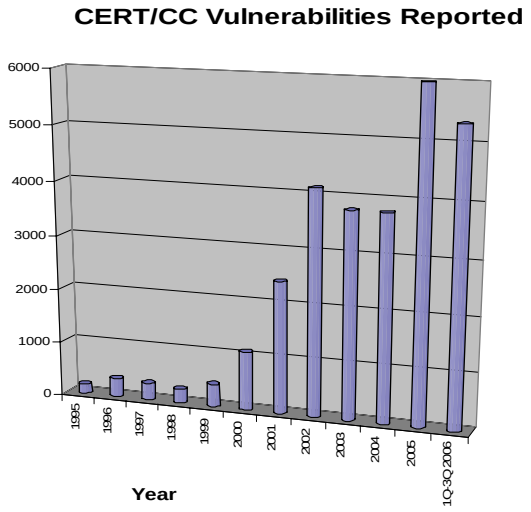

Figure 2: Vulnerability Reports[31]

Interestingly, the Center no longer reports "incidents" on a yearly basis. It stopped reporting in 2004 due to "widespread use of automated attack tools. Attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of the problem. Therefore, as of 2004, we (CERT/CC) will no longer publish the number of incidents reported. Instead, we will be working with others in the community to develop and report on more meaningful metrics."[32] In the sixteen years prior to termination of reporting, the number of incident reports rose from 8 in 1988 to 137,529 in 2003, with over one-half occurring the last four years of reporting.[33] All of these "incidents" come from various origins; some are lone individuals trying to hack into computer systems for the fun of it – to see if they can explore the vulnerabilities to gain fame. Others may be more deliberate, a conscious effort, intended to use the vulnerabilities against another, a possible precursor of an evolving new way to conduct war fighting in the future. This paper explores one such alarming example with a brief

look at China, a nation which is openly engaging in this new form of warfare against the United States.

China's ability to wage cyberwar against the United States is no longer speculation; it occurs daily and is growing exponentially. Two Chinese colonels wrote a paper in 2002 titled *Unrestricted Warfare*, wherein they candidly proposed using cyber attack as a new form of warfare against the United States. In their paper, they analyze United States military power and assess operations over the past decades and conclude "today, the independent use of individual technologies is now becoming more and more imaginable. The emergence of information technology has presented endless possibilities for match-ups involving old and new technologies and among new and advanced technologies."[34] The colonels do not specifically advocate targeting the United States per se, but they are clear on what can be done to wage information warfare against any nation. The colonels state "during a short period of ten years, they transformed from being persons of nameless origins to world public nuisances, with the chief among them being computer hackers…the only thing which could be predicted was that the damage of this type of threat to the large network nation of the United States would certainly be greater than for other nations."[35] These comments serve as an incredible warning and wake-up call.

Maj Gen William Lord, the Air Force's Director of Information, acknowledged that 10 to 20 terabytes of data from the DoD NIPRNET was downloaded by users from China. General Lord, described these coordinated cyber attacks against DOD computers, "as a nation-state threat by the Chinese."[36] The general's statement clearly focuses on a government's coordinated cyber attack program as opposed to lone individuals probing the DOD network. Meanwhile, there are at least twenty nations that also have their own cyber attack programs, and there is no way to know how many terrorist organizations may be launching similar efforts.[37]

Furthermore, a more succinct and to the point report to Congress superbly documents China's views toward cyberwarfare and how China may engage in it against the United States:

> China is moving aggressively toward incorporating cyberwarfare into its military lexicon, organization, training, and doctrine. In fact, if a Revolution in Military Affairs (RMA) is defined as a significant change in technology taken advantage of by comparable changes in military training, organization, and doctrine, then perhaps China of all nations is experiencing a true RMA in cyberspace. Moreover, China's warfare development has [caused] some U.S. military leaders to express concern. The Chinese concept of cyberwarfare

> incorporates unique Chinese views of warfare based around the People's War concept (modern) and the 36 Stratagems (ancient). Both are indigenous views of how to wage war at the strategic, operational, and tactical level. China also is heavily influenced by Marxist-Leninist ideology regarding warfare. Much of its approach has to do with an emphasis on deception, knowledge-style war, and seeking [asymmetric]l advantages over an adversary. Cyberwarfare is seen as a "transformation from the mechanized warfare of the industrial age to . . . a war of decisions and control, a war of knowledge, and a war of intellect." China is pursuing the concept of a Net Force (battalion size), which would consist of a strong reserve force of computer experts trained at a number of universities, academies, and training centers. Several large annual training exercises have already taken place since 1997. The Chinese have placed significant emphasis on training younger persons for these tasks.[38]

The Chinese are actively preparing to fight in intensive information warfare environments. In 2006, more than 8,000 People's Liberation Army personnel took part in a major military exercise which included electronic warfare troops. The 12-day drill, dubbed *Vanguard-206B*, had among its aims, rooting out any existing problems among Chinese troops by exposing them to the most difficult electromagnetic environment. Zeng Weihua, a member of the exercise team stated "the application of information technology is the main purpose of this drill" calling the electromagnetic environment the fifth dimension of warfare and the basis of military actions in modern times. "We want the troops participating in the drill to know that defeat in information techniques means defeat in actual combat," he said.[39] China continues to sharpen its sword in the cyberspace realm, and the US must begin to actively defend itself today to be able to counter this threat.

Today, the East Asia and Pacific region continues to expand its computer manufacturing and by all indications will continue to dominate the market industry in the near future. China is a major manufacturer of both computer hardware and software, with the US increasingly reliant on the components it produces. This raises the specter of the possibility of Asian nations using the manufacturing process as an avenue to launch future cyber attacks against the U.S.

There have been additional cyber attacks against the US from criminal groups over the past decade originating from locations other than China.

Hackers or terrorists operating Russia have successfully penetrated US systems where several incidents demonstrate a well-crafted plan similar to China. In 1998, an attack known as "Moonlight Maze," was traced by DOD officials back to a mainframe computer located in Russia, although the point of origination of the attack was never confirmed. During this incident, officials discovered a pattern of probing computer systems in DOD, Energy Department, NASA, research laboratories and several universities. The event had been occurring for over two years prior to the discovery.[40] The episode also demonstrates a different side of cyberspace, an adversary who went inside computers to collect and steal information instead of causing damage to networks. The attack was a graphic illustration of vulnerable systems, and shows that during conflict, damage to computer systems could cause havoc in the US.

Another case in point, in 2000, a CIA expert testified to a Congressional subcommittee with warnings of foreign cyber threats to the US economic structure. The testimony described a CIA interview with a senior Russian official who proclaimed that an attack against a national target or electrical power distribution could "by virtue of its catastrophic consequences, completely overlap the use of weapons of mass destruction."[41] A 2004 Dartmouth College report depicts an assessment of the capabilities, means and motivations of several selected nation's ability to conduct attacks on the US. In regards to Russia, the study concluded:

> Russia's armed forces, collaborating with experts in the IT sector and academic community, have developed a robust cyber warfare doctrine. The authors of Russia's cyber warfare doctrine have disclosed discussions and debates concerning Moscow's official policy. "Information weaponry," i.e., weapons based on programming code, receives paramount attention in official cyber warfare doctrine. Moscow also has a track record of offensive hacking into Chechen websites. Although we assess it likely that Moscow will continue to scout U.S. military and private sector networks and websites, available evidence is inadequate to predict whether Russia's intelligence services or armed forces would attack U.S. networks, especially after taking into account present-day political and economic ties between the two nations.[42]

Threats to US systems are occurring and growing from other nations, such as Afghanistan, Iran and North Korea, as well. Unexpectedly however, are

the most recent attacks originating from unexpected places such as Canada, Cuba, Italy, Australia, Ireland, Germany, and Iceland. The Israel-Palestine conflict saw a rash of cyber attacks occur when over 40 hackers from 23 countries participated in a cyber war during a four-month period beginning in October 2000, when the cyber battles erupted.[43] Closer to home, a Cuban-born engineer, in a 2006 interview theorized that a dying Fidel Castro could very well launch a cyber attack as a last and final blow against the US. The Castro regime has cultivated cyber warfare techniques for years, and it made the island an electronic spy station first for Russia and then China. Cuba's carefully acquired skill in cyber warfare, its close ties with terrorist groups and terror supporting nations, and first-rate spy services which are operating within the United States, all combine to make Cuba a serious candidate for coordinating a cyber-terror attack.[44]

Based upon the historical data, all indications are future attacks can and will occur from anywhere in the world as computers continue to proliferate globally. These examples demonstrate how cyber warfare has become an attractive alternative to countries not able to engage the US militarily in a traditional conventional war. Tomorrow's cyber war against the US may be conducted by a nation or by a few cyber warriors, just like today's fourth generation wars are being fought by insurgents and guerillas. Before detailing where the Air Force should proceed to defend itself against the threats in cyberspace, a brief look at the history of how the Air Force became dependent on information technology is warranted.

This page intentionally left blank.

Chapter 3
Desktop Computers Become Part of USAF Everyday Life

"Don't expect the typewriter to ever completely disappear."

—Hal Fair, Author[45]

When trying to look twenty years into the future, one must consider what was occurring twenty years in the past. Personnel in the Air Force who have served for the past twenty years have witnessed the rapid integration of computers, particularly desktop computers in day-to-day operations. It is unfathomable for many new airmen to think that until the early 1990s, the majority of *typing* was done on a *typewriter*. The introduction of the desktop computer within Air Force squadrons occurred in the late 1980s, and usually meant a single computer was available for use as a workstation among a group of individuals. Following the rapid advancement of this technology coupled with lower costs, soon thereafter virtually every individual in the Air Force had a computer available.

Acquisition of computers and associated software during this "transition period" in the 1990s was poorly coordinated. Hundreds of various systems were acquired at the wing level to address specific requirements. The necessity to have established standards was recognized, to not only protect computer systems and information, but also to try to standardize equipment and software. While DOD tried to keep up with the pace of acquisition of computer technology, it did not have a good roadmap for the future. Consider a Government Accounting Office (GAO) report fifteen years ago which demonstrated the beginning of a long struggle to try to protect DOD computers and networks:

> The government faces increased levels of risk for information security because of greater network use and computer literacy, and greater dependency on information technology overall. For years hackers have been exploiting security weaknesses of systems attached to the Internet…Between April 1990 and May 1991, computer hackers from the Netherlands penetrated 34 DOD sites. DOD officials, however, are still unable to determine the full scope of the problem because security measures for identifying intrusions are frequently lacking. At many of the sites, the hackers had access to unclassified, sensitive information on such topics as (1) military personnel--personnel performance reports, travel information, and

> personnel reductions; (2) logistics--descriptions of the type and quantity of equipment being moved; and (3) weapons systems development data. Although such information is unclassified, it can be highly sensitive, particularly during times of international conflict. For example, information from at least one system, which was successfully penetrated at several sites, directly supported Operation Desert Storm/Shield. Further, some DOD and government officials have expressed concern that the aggregation of unclassified, sensitive information could result in the compromise of classified information.[46]

DOD, by the mid-1990s, was already extremely dependent on computer systems, and the need to protect these systems became essential to national security, yet vulnerabilities existed department-wide. The DOD computer infrastructure contained hardware and software weaknesses, training deficiencies for individual users and a general lack of a security culture existed. In May 1996, the Defense Information Systems Agency began performing "red teaming" of DOD systems. The Agency was able to electronically break into 65 percent of the systems using commonly available attack tools found on the Internet. Agency officials admitted to DOD that the figure was easily a conservative figure. If given more time, the officials stated that could probably compromise upwards of 95-98 percent of the systems.[47] At this point, an adversary no longer had to get on a military installation and into a building with locked file cabinets to gain access to military information; he simply could electronically gain access to an installation's server to retrieve sensitive files. The GAO ultimately established information security as a government-wide high risk issue in 1997. The GAO continued to issue warnings to all government agencies with at least 54 more reports issued after the GAO's first study in November 1991. These reports all contain a common theme of pervasive weaknesses in cyber defense and security throughout government, and led to intervention at the highest levels of government.

President Clinton, in 1998, attempted to address government cyber vulnerabilities with his critical infrastructure protection policy -- Presidential Decision Directive 63. Clinton's plan contained a national goal that by the year 2000, the United States would "achieve an initial operating capability and no later than five years later, would have achieved and maintained the ability to protect the nation's critical infrastructures from intentional acts to perform several critical functions."[48] The Directive laid the groundwork for structure and organization to prepare for a cyber crisis, but fell well short of a comprehensive and organized government-wide standardization to actively defend the domain.

Five years later, in February 2003, President Bush issued his *National Strategy to Secure Cyber Space* wherein he acknowledged that "securing cyberspace is an extraordinarily difficult strategic challenge."[49] Bush's plan contained three overarching strategic objectives which are similar to those put forth by the Clinton administration. The objectives are to "prevent cyber attacks against America's critical infrastructures; reduce national vulnerability to cyber attacks; and minimize damage and recovery time when cyber attacks do occur."[50] Critics were quick to point out several problems with Bush's plan. Some of the top issues plaguing implementation included a lack of funding sources for the proposed programs and few, if any, incentives or mandatory requirements for private organizations to comply with the plan. Problems with leadership within the National Cyber Security Division are also a major factor for the US being late to task in defense of cyberspace. There have been at least five leaders of the division since its inception in 2003. Other criticism of the division includes failing to set priorities and lack of any developed strategic plans, leaving the nation without a roadmap today.

Today, as in the past, DOD remains in a constant *reactionary* mode to secure itself from cyberspace infiltration. After over two decades of experience in the cyber domain, DOD's improvements have been minimal and there are serious issues that continue to plague DOD when trying to protect its computer systems. Viruses by lone individuals, cyber attacks through intrusion attempts, and more recently, states like China who advocate cyber terrorism against the United States, all can create havoc against DOD systems. A recent example occurred in November, 2006 when Chinese hackers initiated an attack against the Naval War College, forcing the college to shut down its networks. The event also caused US Strategic Command to heighten the DOD's information security alert level.[51] According Alan Paller, the SANS Institutes' director of research, the impact of the event could be severe, with the college most likely needing to replace all the affected computers.[52] The Commerce Department's Bureau of Industry and Security replaced hundreds of computers after similar recent attacks. Chinese attacks on DOD systems are far more widespread than is publicly known according to Paller, because almost all attacks remain classified.[53] While statistics of intrusions on DOD systems are not openly reported, undoubtedly the Air Force has also suffered its share of incursions over the past decade. The lack of a comprehensive defense against the increasing cyberspace threat over the past twenty years provides the backdrop for the Air Force and its vulnerable computer systems and domain it has today.

This page intentionally left blank.

Chapter 4
The Present - The Air Force and Cyberspace, How We Got Here

"As the Air Force embraces this mission area and this domain of operations, somebody may (say) the Air Force is probably the lead for cyberspace…but we are not there yet"

— Lt Gen Michael Peterson, Air Force CIO[54]

The Air Force's Chief Information Officer (CIO), Lt Gen Michael Peterson, has ultimate responsibility over its domain as well as ensuring compliance with DOD and federal regulations governing all activity on AF networks. The Air Force oversees compliance with direction it issues through several instructions and publications. Cyberspace, within the Air Force context, remains a metaphor for key components that constitute the domain, primarily *computers* and the *networks* that interconnect them.

However, this control is not complete. Historically, the Air Force's acquisition of its computers and software was delegated to the wing level, and is still the same today. The cheapest method to do so traditionally has been to acquire commercial off-the-shelf (COTS) products offered by numerous private businesses. The overwhelming majority of the computers contain operating systems produced by Microsoft, but depending on a wing's particular needs, may be a different system.

The Air Force is currently working to move its information systems into alignment with a new data strategy developed by DOD. The DOD strategy requires services to follow certain standards developed in order to facilitate information exchange amongst the services. The problem the Air Force is facing, according to Lt Gen Peterson, is the difficulty with compliance due to the number of legacy data systems the Air Force is already relying on – systems not necessarily compliant with DOD's net-centric data strategy.[55] The general's statements echo the reports described in the previous chapter, however, a closer look at how the Air Force arrived in this condition is warranted.

During the 1980s and 1990s the Air Force began expanding its use of computers throughout the service, about the same time most of America was being introduced to the World Wide Web. This period marked the beginnings of an integrated arrangement of the Air Force's computers, but was far from being capable of working as a centralized network that devolved into today's NIPRNET. Additionally, at the time, there was no consensus on what systems would work best. Computer networking was a wide-open competitive field with multiple concepts, each with its own advantages and disadvantages. The Air Force provided overarching guidance to each wing during this time period, however major commands focused on implementing networks that helped accomplish the specific mission for which each command was responsible. The process allowed the Air Force to rapidly

expand into the computer arena, but consequences remain today. The lack of standardization Air Force-wide during implementation of the domain over the past decades means the Air Force relies on each base to defend its own network. A weak link at a particular base will allow an intruder the ability to penetrate not only that base, but potentially create havoc across the entire Air Force network. The Air Force is a long way away from being able to provide a robust defense with the ability to *centrally* control and defend the entire network during a cyber crisis. Meanwhile, several attack methods are available to an enemy with the desire to exploit the Air Force's network.

Attacks in cyberspace may come from one of three main channels of attack that exist — *through cyberspace*, such as via worms or other malware, by direct *destruction or alteration of physical structure*, such as buildings or telecommunications lines, or through intentional or inadvertent *actions by a trusted insider*.[56] While all three types of attack can each have devastating effects individually, and would have catastrophic impact together, the focus of this paper is toward the cyberspace aspect. This paper is specifically focused on the defense of the Air Force's 525,000 computers purchased through various vendors throughout the world.

One of the first steps in creating a defense on a computer network is to analyze the susceptibility of the computer hardware, or the "guts" of the all computers. The computer hardware components are most likely manufactured and assembled somewhere in Asia, perhaps even in China. Software, to include the basic operating system of the computers, comes already loaded, rendering the system "ready to go" for the customer. Perhaps the software was created in another country in Asia, such as India, the leading software manufacturer in the world. Microsoft has five research laboratories, one located in Bangalore, India and another located in Beijing, China. The China center of excellence, touted by Microsoft as "the world's hottest computer lab," is focusing its research on, among other things, networking and systems.[57] Obviously, Microsoft puts significant emphasis on the research conducted in China, as described on its website: "this lab harnesses the best talents from across the world to realize Microsoft's vision of computing and push the state of the art. With more than 300 researchers and over 1,200 top-tier publications, the lab has grown into a center of excellence for cutting-edge research."[58]

As discussed earlier, acquiring both hardware and software components from potential US adversaries is an ominous set-up and certainly a potential for disaster from the beginning. Suppose, for example, the construction of a new computer includes the adversary installing a device inside the computer, such as a "harmless" extra chip, allowing that enemy to identify the computer as being on the military domain. This chip sends a signal to the enemy identifying itself, wherefrom they are able to capture the information on the hard drive, then are able to retrieve the data via the internet. This may be the easiest way to penetrate any aspect of the DOD domain. Another approach is known as a *back door*[59] in the computer industry and is a means of access

through software into a computer program bypassing security mechanisms. Programmers may install back doors in software so the program can be accessed for troubleshooting or other purposes. Likewise, an adversarial country may use back doors placed inside during software production as part of an exploitation plan. Suppose Microsoft developers in China included any of these during their research.

Does anyone ever check to see what the manufacturer has put *inside the computer* prior to loading military information – or better yet, prior to connecting to a base communications network? This may appear to be a logical, even rhetorical question but it remains very relevant to the basic security of the Air Force's cyberspace domain and it should be asked on a regular basis. The typical Air Force computer arrives in the workplace at the local level, as each base purchases COTS computers and usually through the lowest bidder/best price method. Once the computers arrive at the local communications squadron, additional software is loaded onto the computer. A squadron's information manager installs the computers and the connected user is now on the base's network, and indeed the entire military domain. The computer, now available for the enemy to enter, is potentially susceptible for attack and exploit.

Consider a report by leading security experts for computer and internet security: "recent data shows that 90 percent or more of the attacks or incidents against systems have taken advantage of known vulnerabilities with known solutions (e.g. patches or configuration options). In fact, it is typically reported that most attacks are based on a relatively small number of reported vulnerabilities."[60] The decentralized process is responsive at the local level and works well; however, this provides the opportunity for vulnerabilities to be exploited, and DOD acknowledges this danger. The Air Force acquisition process over the past few decades lacked standardization during software and hardware purchases, exasperating the weaknesses. Additionally, there are too few security safeguards to protect the cyber environment especially with the exponential growth of both capability and associated risk as the Air Force's domain continues to grow.

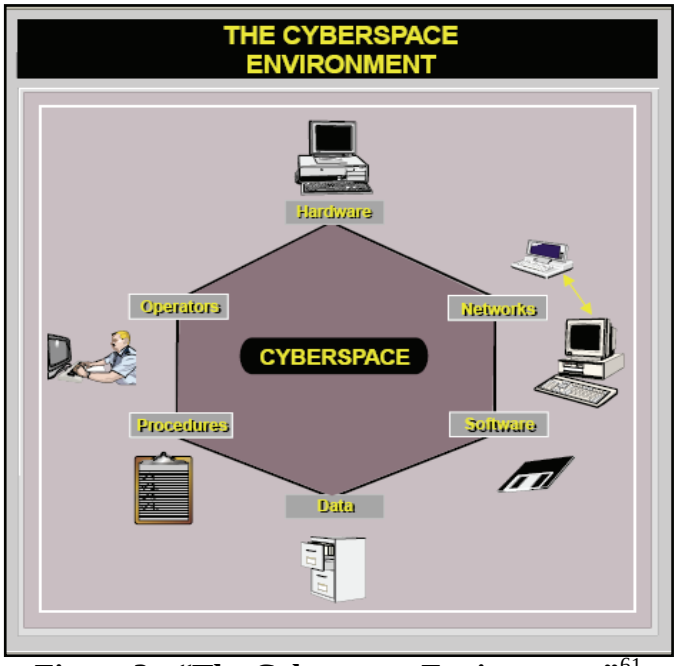

Figure 3: "The Cyberspace Environment"[61]

Analyzing the cyberspace environment depicted in Figure 3, it is easy to see the six main areas that DOD recognizes as critical components of the cyberspace domain. Three of the areas; the human operators, procedures, and data are pretty well controlled within the Air Force. Operators are basically any person within the Air Force who is given access to a computer and procedures are established and controlled by DOD to make sure that access is limited to authorized personnel, and that the computer is physically controlled. Data is controlled by the Air Force, permitting authorization of what goes *into* the computer. The three remaining areas, software, networks and hardware, remain a significant vulnerability concern in the Air Force not only today, but more importantly, in the future.

Reaction from a 2003 GAO report prompted a response from security experts proclaiming the *DOD relies too much on commercial software, does not know who is creating the software that goes into the computer, and ultimately faces several cyber security problems.*[62] One expert, Professor Eugene Spafford, the director of the Center for Education and Research in Information Assurance and Security at Purdue University, questioned the COTS software produced outside the United States in his testimony to a US House of Representatives subcommittee. Tackling the use of COTS head-on, Stafford stated "much of this software, an increasing amount of this software, is being written by individuals we would not allow into the environments where it's operating…they're not US citizens…they don't have the kind of background checks." Stafford further stated that using the software, for computer systems containing national security information may be questionable. "It introduces a tremendous vulnerability to our systems – the

software being developed, sometimes tens of millions of lines, by individuals whose motivations and agendas may not be fully known."[63]

DOD uses the same software across many of its systems, wherein many of the software products suffered about 2,000 vulnerabilities in 2002. This forces operators and administrators to apply three to five security patches every week. DOD continues, at the same time, to try to defend its computers against hackers. DOD blocked and traced 60,000 intrusion attempts on its unclassified networks in 2004, and continuously wrestles with spam, illicit pornography and other common internet threats.[64] Cyber attacks usually happen very quickly and often with great stealth. Critical war fighting operations must continue to function effectively while under cyber attack. This problem is not unique to the Air Force and DOD has effective agencies to help.

The Air Force gets assistance from DOD, including the Defense Information Systems Agency (DISA), which helps shape the Air Force's own guidance and directives. DISA's mission as a combat support agency includes the responsibility for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DOD components, under all conditions of peace and war.[65] The DISA Director is dual-hatted as director of United States Strategic Command's Joint Task Force-Global Network Operations. He directs the operation and defense of the Global Information Grid to assure timely and secure Net-Centric capabilities across strategic, operational, and tactical boundaries in support of DOD's full spectrum of war fighting, intelligence, and business missions.[66] The Task Force is also responsible for the DOD Computer Emergency Readiness Team, which provides protection and defense of DOD information and information systems.

Additionally, DISA's Information Assurance/NetOps Program Executive Office manages DOD information assurance and network operations capabilities. The office provides responsive, secure, and interoperable net-centric solutions necessary to secure and operate the GIG in support of the Secretary of Defense, Combatant Commanders, Joint/Combined Task Forces, Services, and Agencies.[67] The Air Force also takes several steps to protect the cyberspace domain with some of these DOD-wide processes in place. When the Air Force stood up the Cyberspace Task Force in early 2006 and declared cyber a war fighting arena, the next step was to organize itself to conduct operations in this new field.

The Secretary of the Air Force, in November 2006, announced that Eighth Air Force would be the command responsible for cyberspace, a major step towards fulfilling the new mission. Eighth Air Force will develop the Air Force's future roadmap in the cyberspace domain and will organize, train and equip the Air Force as it prepares for operations in cyberspace. A major part of the mission is to secure the cyberspace domain by denying an adversary the ability to exploit that same domain. The Secretary of the Air Force stated that

"the aim is to develop ultimately a Major Command that stands alongside Air Force Space Command and Air Combat Command as the providers of forces on whom the President, Combatant Commanders and the American people can rely for preserving freedom of access and commerce in Air, Space, and, now, Cyberspace."[68]

The stand-up of the command, while new for the Air Force, is not necessarily unique for DOD. The Navy, for example, established a similar command to be the single point for consolidating requirements to provide secure operations within its service. The Naval Network Warfare Command is the Navy's central operational authority for space, information technology requirements, and network and information operations in support of naval forces afloat and ashore. The command's mission is to operate a secure and interoperable naval network that enables effects-based operations and innovation. Also, the command coordinates and assesses the Navy operational requirements for and use of network/command and control/information technology/information operations and space. It also serves as the operational forces' advocate in the development and fielding of information technology, information operations and space.[69] The Air Force quickly picked up on the Navy's approach of providing necessary technology to their users while simultaneously ensuring a secure network.

The Air Force's newest security measure began in early 2006 when it implemented the first Standard Desktop Configuration as part of an effort to reduce confusion amongst a multitude of software systems. Moving to the configuration will also provide a strong measure to enhance the security of the Air Force network. The desktop configuration, part of a five-year, $70 million contract with Microsoft, establishes Windows XP as the standard operating system and provides a core set of office automation tools such as Office 2003, Internet Explorer, Acrobat Reader, ActiveCard Gold, ICS Viewer, Norton Antivirus and more.[70] This is one of the first steps the Air Force has taken to reduce the number of intrusion attempts, numbering in the tens of thousands, it counters each year. Air Education and Training Command's Network Operations and Security Center Engineering and Test and Evaluation chief stated "when the configuration is standardized, security will be increased exponentially through more effective centralized management of the security posture. Our goal is to plug security vulnerabilities in hours versus the weeks it takes us today."[71] This is an important step for cyber defense by setting standards for all Air Force computers. This step will hopefully be the catalyst for future security efforts, but the Air Force is also conducting a major effort at one of its research laboratories.

The Air Force Research Laboratory (AFRL) accomplishes its mission of "leading the discovery, development, and integration of affordable warfighting technologies for our air and space forces."[72] AFRL has nine technology directorates scattered throughout the United States, one of which is an Information Directorate, located in Rome, New York. A Cyber

Operations Branch within the directorate fulfills its mission of supporting the full spectrum of Air Force cyber operations capabilities, from peace through crises and war and back to peace. The branch applies information technology across the full spectrum of cyber operations, in support of Air Force mission requirements. It also provides research and development in the areas of computer and network risk assessment/management, vulnerability assessment, assurance techniques, detection of intrusions and misuse, network security, wireless information assurance, assessment of information damage, cyber forensics, recovery of information systems and computer networks to operational levels, and a full spectrum of active response and computer network attack techniques.[73]

The Center for Information Security and Education and Research (CISER) within the Information Directorate, has the mission to "develop Air Force and DOD leaders in cyber operations expert in the use of doctrine, techniques, and technologies that ensure dominance and superiority in cyberspace."[74] CISER research areas include Cyber workforce development, insider threat mitigation, network attack, defense, and exploitation, cyber targeting and attribution, autonomous and distributed sensors, wired and wireless communications, software vulnerabilities and protections, secure and anonymous communications and biometrics.[75] When questioned about a timeline for implementation of the research areas, engineers admitted they may still be working on these issues 10 years from now, as these engineers are concerned with the lack of a long-term vision within the U.S. in the cyberspace arena as well as a dearth of

The engineers were concerned regarding the alarmingly small number of personnel within the Air Force, less than five percent, who possess computer related degrees. Now, as well as in the future, the Air Force will face problems trying to recruit personnel within the US if it tries to add more expertise in research laboratories. Trends show Science and Technology education in the US, particularly Computer Science majors at universities, were down by 23 percent in 2003. On the other hand, statistics show 58 percent of China's undergraduate degrees in 2002 were in the science and technology areas.[76] The computer industry is moving research centers toward the Asia region due to these developments, something the Air Force cannot do.

The President's Council of Advisors on Science and Technology, in a 2004 report, reinforces CISER's worries. The group's report to the President spells out their findings:

> "Additional concerns arise from US education trends. Recent statistics have shown an increase in foreign students as a share of science, mathematics and engineering degrees at all levels. This development coincides with an increased tendency of these foreign graduates to

> receive these degrees in their home countries. These trends buttress not only the abilities of other countries to attract outsourced manufacturing, but also their desire to match the US pre-eminence in leading-edge R&D and design."[77]

The report reinforces CISER engineers' fears that US students are turning away from the S&T careers while students from foreign countries are focusing in this area.

Meanwhile, the downward trend in expertise in the career field along with Asia's strong emphasis on educating and developing more of their population is unsettling. The question will be: will the US dependence on technology force us to become dependent on other countries? Statistics show that this will be the case, all at a time the Air Force has a growing dependence on the cyber domain which will likewise rapidly increase in the future.

Chapter 5
Off We Go to the Wild Blue Yonder

"Thinking about the future increases the likelihood of success in the long run."

— The Future Belongs to Those Who…A Guide for Thinking about the Future [78]

This author spent countless hours on the internet, ironically enough, researching information on studies for work on *computer defense* focused beyond 10 years, for *any* type of data whether it was from commercial industry, military, and perhaps even from international countries. Surprisingly, little information on computer defense exists for the 2030 timeframe; it appears most research is focused on the nearer term of less than 10 years. For example, an April 2006 report titled "Federal Plan for Cyber Security and Information Assurance Research and Development" by the National Science and Technology Council focuses on cyber security and defense, but is clearly focused on the near term.[79] Interviews with AFRL staff reveal the reason perhaps is due to the expectations of so much change over the next 20 years; no one is willing to invest the effort to defend the "unknown." Regardless, described below are three different cases of research areas, all focused towards 2030.

The first research effort underway is very promising, and is within the Air Force's Research Laboratory. The author met with Dr. Kamal Jabbour, Principle Computer Engineer, who is the technical lead of the cyber defense research program and Maj (Dr) David Bibighaus, Cyber Operations Branch Chief, during a September 2006 visit to the AFRL Information Directorate's Cyber Operations Branch located in Rome, New York. The purpose of the meeting was to discuss the focus of AFRL's future cyberspace research programs underway. Dr. Jabbour and Maj Bibighaus, during discussions on the topic of an integrated cyber defense, assessed the current capability as *threat/attack reactive*, meaning the Air Force has an "awareness of cyber attacks once they affect Air Force installations and assets."[80] Additionally, they assess Air Force capability as follows: "we cannot see the attack coming; we have limited understanding of the threats; attack attribution to the source is very difficult; our only defense is within our boundaries; we have limited detection and prevention malware; combating an attack can result in the loss of mission capability and denial of service; and finally, recovery process from an attack is done manually."[81] Their assessment is particularly disturbing as it confirms that actions today consists of *reacting* to any and every threat – and confirms the fact that something must be done to protect the cyberspace domain now to protect the future. The Air Force must take measures to aggressively defend its domain today; a failure to do so will greatly inhibit its ability to keep up with rapid changes. An active defense of cyberspace is imperative, as the US will fall behind to its adversaries due to its failure to look towards future threats. In the future, information technology will

continue to progress at exponential rates, driven primarily by the private sector needs, not by the US government. This swift expansion means our adversaries can, and will, upgrade their capabilities faster than government agencies can – presenting even more of a dilemma for DOD.

AFRL Cyber Operation Branch's future vision is to proactively defend cyberspace. They intend to do so by engaging and acquiring advance situational awareness of an adversary's cyber intent. The vision also includes engaging, if possible, outside of our cyber borders protecting the information, for both hardware and software. The goal is to protect all platforms against corruption and manipulation and utilize adaptive, self-organizing, self-healing resources, all of which will enable full mission operations.[82] The branch's research efforts are toward the future, and one of the most promising ideas led to a notion coined the "Cybercraft".

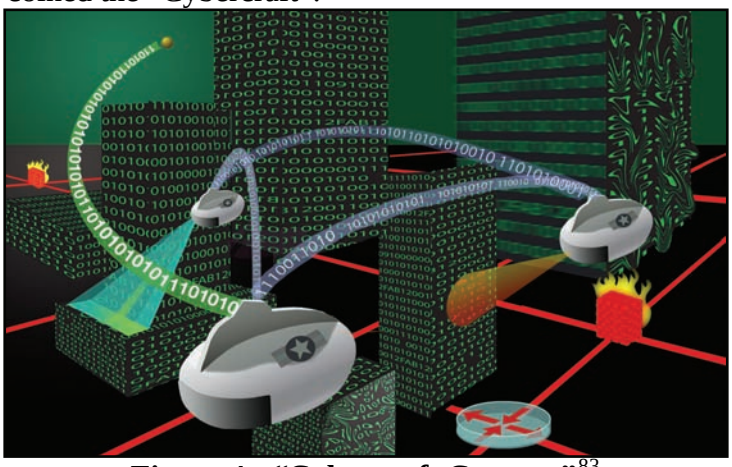

Figure 4: "Cybercraft Concept"[83]

Cybercraft, a software device which could be installed on every electronic medium in the Air Force, is a new research concept where the Cybercraft acts autonomously to *actively* defend military information systems. The Cybercraft's mission is to provide continuous defense of any piece of equipment connected to the Air Force's cyber domain, including all hardware and software. The significance of the Cybercraft technology is remarkable due to the device being one of the first in the industry that actively seeks out "trouble." The craft are centrally preprogrammed by administrators – initiating any foreign hardware or software into the domain different from that pre-planned causes the Cybercraft to immediately raise warning flags. Additionally, Cybercraft have the ability to not only protect a computer from corruption and manipulation, but are able to isolate a computer if a previously unrecognized threat arrives. Perhaps just as important, the Cybercraft concept permits the Air Force to centrally control its entire domain from a single location. The design allows complete access to the entire network of Air Force computers via the Cybercraft within seconds.

These craft were designed with four objectives in mind. They are *simple* (consistent design), *scalable* to fleet sizes of over 1 million, *reliable* (no single point of failure), and *provable*.[84] Also, researchers compare several qualities

of the Cybercraft to an aircraft weapon system. The Cybercraft, like an aircraft, is to be commanded, controlled, has communications capability and carries payloads that cause effects. Furthermore, Cybercraft is designed to have a long service life; be able to handle a variety of missions; be able to handle intense scrutiny; have rapid deployment capability, to be expendable; have specific effects; and be highly effective. The concept appears to be very promising and initial tests proved the concept is feasible. However, Dr. Jabbour and Maj Bibighaus acknowledge the difficulty in creating and fielding the concept Air Force-wide, wherein they estimate it as a "long term" project, meaning the Cybercraft would be in use by the 2015 to 2020 timeframe.

A second research effort, which the Air Force should monitor, recently began in the Navy. The Navy, just like all the other services in the military, protects its information domain through robust defense mechanisms. The Navy's Cyber Defense Operations Command relies on PROMETHEUS, a web-based solution that monitors, reports and thwarts malicious network activity. The Command's nerve center, using PROMETHEUS, analyzes masses of incoming and stored data on the Navy's domain. The Command can also watch for probing activity or precursors indicating an attack may occur in the future.[85] However, the Navy's defense system is akin to every other service in DOD which protects its network grid by using firewalls, anti-virus products and analytic solutions to monitor for attacks and react accordingly. The Navy's method of cyber defense is another case in point which shows the necessity to develop active defenses within DOD.

Nevertheless, the Navy, just like the Air Force, acknowledges the importance of cyberspace as a warfare domain of the future, and recently began looking at cyberspace toward the *2030 timeframe.* A Navy research group is actively looking at the future, much like the Air Force's Blue Horizons study. Admiral M. G. Mullen, Chief of Naval Operations, on 16 October 2006, sent a memorandum to the Director, Strategic Studies Group, located at the Naval War College, and tasks the group to "generate revolutionary naval concepts to ensure Navy capabilities in this emerging warfare domain in addition to our traditional domains."[86] Additionally, the admiral asked the question "what will warfare be like in cyberspace?" and then gave several potential aspects to consider "identifying aspects of change that have been neglected or dismissed" and to "examine Navy culture – identify aspects that should be preserved, protected, and those that interfere with our ability to see, recognize, and adapt to future challenges."[87] Admiral Mullen concluded his memo requesting a "high-level blueprint that encompasses a longer-term view as well as a roadmap that includes immediately actionable steps…that our Navy may take to begin developing the capabilities you envision."[88] At this time, it appears the Air Force and Navy are taking the lead inside DOD to prepare for conflict in cyberspace.

The growth of information technology is occurring at such a rapid rate and commercial industry is forced to concentrate the majority of its efforts on

short term issues. This trend is causing a lack of focus towards futuristic cyberspace research, with even less attention on the defense of the cyber domain. One area many experts are focusing their attention towards the future is in quantum computing. These new computers, with previously unheard of calculating power, are in their infancy today but will likely be available by 2030. This new method of computing power will offer tremendous capabilities, but will also be very dangerous in the hands of an adversary. Most security systems installed by the world's vital institutions, including banking, commerce and government, have come to depend on current encryption methods, which against quantum computers, would become obsolete.

Quantum research is underway in several countries, with national government and military agencies providing funding support. Already, experiments have occurred in which quantum computational operations were executed on a very small number of qubits.[89] Today, the US has the lead in quantum research, but competition from Europe, Japan, Australia, and China is strong and growing. Other types of futuristic research in the commercial sector are few and far between.

Chapter 6
Analysis and Recommendations

"Any attempt to predict the future security environment of 2025 is inherently difficult. Given the dynamics of change over time, we must develop a mix of agile and flexible capabilities to mitigate uncertainty."
—CJCS Assessment of 2006 QDR[90]

Analysis of the Future

All indicators point toward cyberspace having exponential growth over the next 20 years. Computer technology is advancing so fast the Air Force's chance to have any credible defenses of its domain will be left in its dust. At the same time, the Air Force cannot afford to wait any longer to create a proactive defense of its networks. A country that develops a quantum computer will enjoy a significant advantage in both the civilian and military worlds; therefore research is being conducted at a frantic pace. Quantum computing capability would create the ultimate cyber weapon, creating the potential for world chaos. Any country able to gain a breakthrough could do severe damage to the Air Force's cyber domain with the current *reactive* defenses in place. A quantum computer would essentially have the ability to break every password and security code and get inside any computer in existence today. An adversary armed with a quantum computer would be able to acquire data, search files and move on to his next target with ease. A reactive defense, pretty effective in the past, should not be the Air Force's primary solution to defend itself. Turning toward the future, the Air Force not only needs to take care of today's cyber defense needs, but must prepare for the defense of the rapid expansion of newer technology, such as quantum computing. The Air Force must defend its cyber domain in the future using active denial methods.

The previous chapter described how the US commercial industry is not particularly focused on ideas toward the 2030 timeframe. One reason is the US is losing ground for technology experts to conduct research in these areas, but the opposite is true for countries who consider information technology research a priority. Statistics from the National Science Board's 2006 report on *Science and Engineering Indicators* is one example of a trend which will influence the US ability to conduct research 20 years from now. In this case a downward trend is noted as new US college students shy away from the technology career field. This statistic is matched against a decline in the number of people with advanced degrees – and experience, who will retire in the next few years. According to the Board's data, just under one-third of all US degrees are in science and engineering, and this number continues to decline. In the meantime, as Figure 5 shows, the number of engineering degrees awarded in Asia was *four times* as much as in North America.

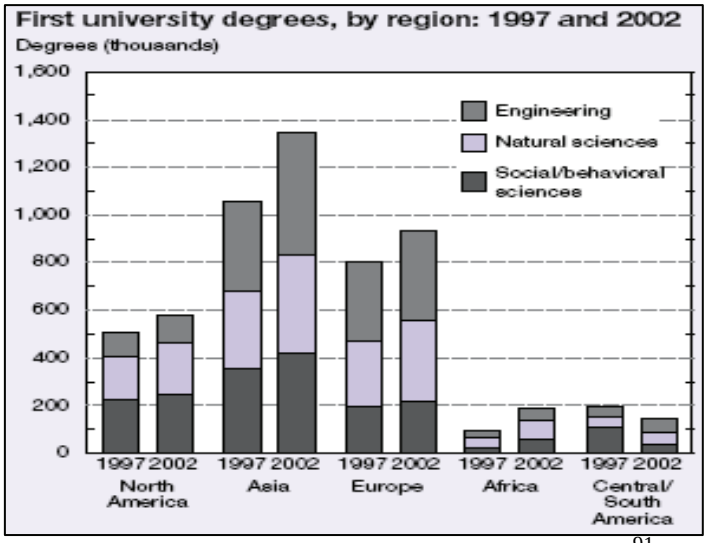

Figure 5: First University Degrees, by Region[91]

During the past two decades two-thirds of foreign students earning a US science and engineering doctorate degree were from Asia: about twenty percent from China and approximately ten percent each from Taiwan, India, and South Korea (Figure 6).

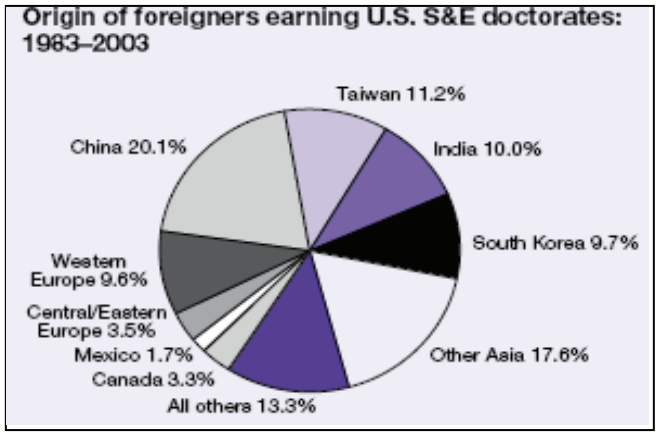

Figure 6: Origin of Foreigners Earning US Science and Education PhDs[92]

Many retirements from the US science and engineering labor force are impending. Barring major changes in current trends, many individuals in the labor force will retire in the coming decades. In 2003, thirteen percent of science and engineering bachelor's degree holders, twenty percent of master's degree holders, and 28 percent of doctorate holders were 55 years old or older. Historically, by age 61 about half of the bachelor's degree holders no longer work full time; the same is true at age 62 for those with master's degrees and at age 64 for doctorate holders.[93]

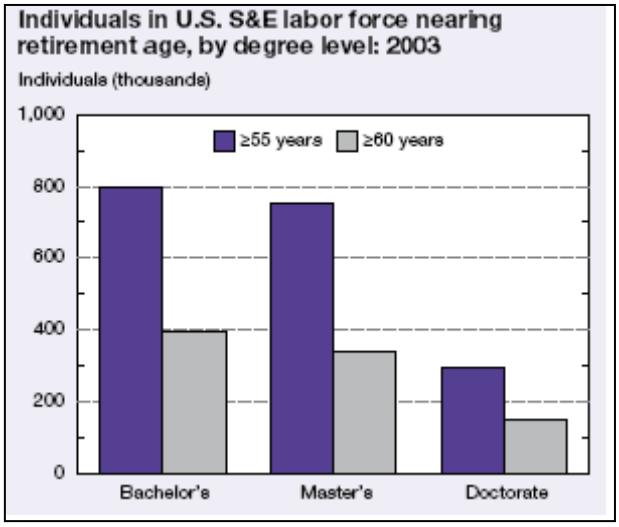

Figure 7: Individuals in US Science and Engineering Force Nearing Retirement[94]

The information all point to disturbing statistics if the Air Force is going to take and sustain the lead of defending cyberspace in the future. The Air Force will compete not only with the other military services, but the lucrative commercial market as well, for the limited graduates in this advanced career specialty.

Historical data, as we have seen, points to a very vulnerable DOD network, defended by reactive measures, which cannot continue with the military's significant reliance on cyber space. Rising at an even more alarming rate are the threats to the domain. Steps must be taken today to focus research on a proactive defense of the Air Force's cyber domain. The author presents recommendations for the Air Force to consider when in order to defend its cyberspace domain now and in the future.

Recommendations

The Secretary and Chief of Staff of the Air Force brought cyberspace to the forefront of the Air Force mission. The Air Force must rapidly move cyberspace from its infancy to maturity in order to succeed in this new mission area. This paper skims some of today's potential vulnerabilities, many of which are already known not only by the Air Force, but by future adversaries. The Air Force must not only solve the dilemma faced by the current threats, but must anticipate the future in order to defend its domain to maintain the freedom of cyberspace. To ensure cyberspace security in the 2030 timeframe, the following recommendations are offered:

1. *The Air Force should aggressively pursue AFRL's cybercraft concept as a hedge for increased defense of its cyberspace domain.* The cybercraft is just one example of forward-looking research towards the 2030 timeframe. It is critical that the Air Force stop relying on a passive defense stance to protect its network. The cybercraft concept is a step in the right direction, and not only provides an active defense, but can be controlled at a central location. The centralized control allows greater visibility throughout the

chain of command, as well as provides a "mothership" in which the Air Force can have virtually instantaneous control over its domain, all the way down to individual computers. AFRL estimates the ability to field its cybercraft, *without additional help*, in about 10 to 15 years.

2. *DISA's PEO-IAN office should pursue technology to actively scan the GIG as part of its Computer Network Defense (CND).* This recommendation is consistent with one of the seven functions within the PEO-IAN office. Specifically, the office states that it "develops/acquires and implements enterprise wide CND solutions and integration approaches to identify threats to the GIG, sense network and host-based attacks/degradations, and *develop/disseminate countermeasures* and courses of action.[95] Scanning the GIG provides a defense mechanism prior to reaching the actual computers, and would compliment AFRL's cybercraft concept. A timeframe of completion for this project is unknown at this time.
3. *As the Nation takes steps to improve the security of current systems, it must also ensure that future cyber systems and infrastructure are built to be secure.* This will become increasingly important as more and more of our daily economic and physical lives come to depend on cyber infrastructure. Future security requires research in cyberspace security topics and a commitment to the development of more secure products. COTS hardware and software undoubtedly is the most cost-effective means for acquisition of computers and computer systems. The Air Force should thoroughly examine products it purchases from commercial industry in order to ensure security from the origin, which would help minimize the threats today. Since many computers and computer systems have a five to ten year life in the Air Force, this would help protect the domain in the near term. Unless the AF establishes processes now to review new purchase procedures, there is no way for the Air Force to protect hardware and software in 2030.
4. *The Air Force should consider partnerships with its sister services, other government agencies, non-government organizations and non-military authorities in an effort to keep cyberspace secure.* Cyberspace is a domain wherein the Air Force has taken the lead to operate in, therefore is should use all means to keep open communication on identifying security risks and vulnerabilities on computer hardware and software along with the internet. Additionally, the Air Force should actively work to explore any governmental or commercial research efforts underway that focus toward the 2030 timeframe. DOD already has systems in place to share information, but often does not get to the lowest level expediently – often days pass before vulnerabilities are identified *and corrected* wherein information can be stolen or corrupted. The author was unable to find information to show DOD is looking forward towards the 2030 timeframe during research.
5. *Coordinate the efforts of Blue Horizons with the Air Force Cyber Command.* Since cyberspace is a focus area of the Blue Horizons study

and the Cyber Command is in its infancy, establishing connections between the two offers great potential. The Cyber Command should consider the research conducted by Blue Horizons when planning for the future of defense of the Air Force's cyber domain.

This page intentionally left blank.

Chapter 7
Final Assessment

"All of our experience is with the past, but all of our decisions are about the future…the first step in thinking about the future involves exploring trends that are already underway."

—The Future Belongs to Those Who…A Guide for Thinking about the Future[96]

The DOD maintains the largest computer network in the world. Connecting thousands of IT systems around the globe, the DOD's computer network is critical for the command and control of each branch of the US military. Exploring *defense* of the DOD's cyberspace domain in 2030 was clearly a challenging endeavor, but as reinforced by the conduct of this research, is vitally important. This research project began with an idea there would be plenty of futuristic thinking in the cyberspace area. This author conducted research primarily in open sources, which was intentional, in order to keep the effort unclassified. The intent of conducting unclassified cyberspace defense research was to look at a broad range of activity both within and outside the Air Force, specifically focused 20 years or more in the future.

A visit to the AFRL Information Directorate revealed promising work being conducted in the cyberspace area with a vision and focus on security and defense that this author strongly believes warrants further attention. The author was somewhat surprised to discover that the Navy has undertaken its own study of cyberspace focused on the 2030 timeframe. This recent study, which will be conducted by the Navy War College, appears to parallel the study ongoing by the Air Force's Blue Horizons group. The author recommends that the Blue Horizons monitor, and perhaps coordinate with the Navy as Blue Horizons continues its cyberspace research. Finally, there is little information on future research being conducted in commercial industry. This suggests very little is being done in the commercial sector with a view toward the long-term threat, though research on near-term problems continues, and breakthroughs in this area occur frequently. For example, in January 2007, Microsoft released its new operating system, called *Windows Vista*. Security was the main focus during development of the software in order to improve the computer's overall basic protection. Microsoft's previous operating systems contained numerous security vulnerabilities, which were very susceptible to malware and viruses, necessitating the installation of various countermeasures in order to make the basic computer safe. Microsoft's vision during the development of *Vista* was to close many of the security gaps in previous operating systems. The fact that commercial companies, such as Microsoft, are turning their focus toward actively defense of computers is a positive sign, and hopefully points toward a trend in the future in industry. Without a doubt, the Air Force will continue to rely on the

commercial market for its computers and associated software for the next 20 years, and should champion companies who design secure components.

The Air Force should pay attention to the future of quantum computing, and concentrate equal attention to defensive measures. Research in quantum encryption capability is a necessity in order to secure not only the Air Force's cyber domain, but all passwords and codes associated with it.

The future of cyberspace is very exciting, as the Air Force works out its new mission. Cyber attacks occur daily, yet most of us get used to them, as we assume that a forthcoming solution will counter the threat. It is easy to overlook the fact that a well planned and executed cyber attack – from only a small group of persons, much less another country – could paralyze our military. The Air Force's legacy systems, purchased over the past decades, must be upgraded and synchronized in order to tighten security loopholes which still persist today. This paper clearly illustrates how well-planned, coordinated attacks continue to occur throughout DOD even with numerous safeguards implemented during the same timeframe. Alarmingly, today's attacks may be the tip of the iceberg and perhaps are the precursor for even greater and more devastating assaults lurking in the future.

We must begin by securing cyberspace within the Air Force in order to meet the Secretary Wynne and Gen Moseley's vision. The Air Force Cyber Task Force must articulate a clear strategy for the future in cyberspace, paying close attention to the protection and defense of the domain. Preoccupation by the current capability in cyberspace, while necessary, is also hazardous. The Air Force must consider the effects of cyberspace in the future, and should consider the fact that this domain may be the weapon system of choice over the next 25 years. We must expect that future adversaries will use any tool or method to challenge the unrivaled military capability of the US. The time has come to implement an active defense in the Air Force's cyber domain.

Ray Kurzweil's futuristic novel, *The Singularity is Near*, provided this author with the idea of researching the *defense of cyberspace*. Consider this quote from the book: "by the late 2030s and 2040s, as we approach human body version 3.0 and the predominance of nonbiological intelligence, the issue of cyberwarfare will move to center stage. When everything is information, the ability to control your own information and disrupt your enemy's communication, command, and control will be a primary determinant of military success."[97] This effort began with these thoughts in mind, along with the thesis that defense of the cyberspace domain would be a top priority for the future. Also, along came an expectation that there would be several sources of information from which to conduct research in the 2030 timeframe. Surprisingly, this research effort over the past several months proved otherwise. Although undoubtedly there are more long term efforts underway than what is described in this document, interviews and discussions show an alarming trend that looking at the future 20 years is basically not worth the effort. Personnel conducting research in cyberspace defense are not only unsure of what cyberspace will be in the next 20 years, they are even less

certain of how to defend it. The author concludes that futures study groups, such as Blue Horizons, are absolutely imperative for the Air Force as few organizations aggressively look at the future.

Bibliography

"Consensus Minimum Security Benchmarks", Fall 2002 Newsletter, http://iac.dtic.mil/iatac (accessed 29 Sep 06)

56th Communications Squadron, Air Force News Statement, 16 Jun 06, http://www.luke.af.mil/news/story_print.asp?storyID=123031316 (accessed 3 Dec 06)

Air Force News Statement, 9 Dec 05, http://af.mil/pressreleases/story_print.asp? storyID=123013463 (accessed 29 Sep 06)

Air Force News Statement, 9 Dec 05, http://af.mil/news/story_print.asp?storyID=123026382. (accessed 29 Sep 06)

Air Force Research Lab, *"Air War College Blue Horizons Orientation"*, site visit to HQ AFRL, Wright Patterson AFB, OH, 29-30 Aug 2006

Air Force Research Lab, *"Air War College Blue Horizons Orientation"*, site visit to AFRL Information Directorate, Rome, New York, 11-13 Sep 2006

CERT/CC Statistics, http://www.cert.org/stats/cert_stats.html (accessed 1 Dec 06)

Clark, Richard A., Testimony to the Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, 8 Apr 03

CRS Report to Congress, *"Creating a National Framework for Cybersecurity: An Analysis of Issues and Options"*, 22 Feb 05

CRS Report to Congress, "*Cyberwarfare*", 19 Jun 01,12

Department of Defense, *Quadrennial Defense Review (QDR)*, 6 Feb 2006

Fair, Hal, http://www.quotatio.com/f/ (accessed 2 Dec 06)

Federal Plan For Cyber Security and Information Assurance Research and Development, Apr 2006

The Free Dictionary web site, http://www.thefreedictionary.com/cyberspace (accessed 30 Sep 06)

GAO Report, *Computer Security Hackers Penetrate DOD Computer Systems (GAO/T-IMTEC-92-5)*, 20 Nov 91, accessed through Global Security.org website, http://www.globalsecurity.org/security/library/report/gao/145327.pdf

Gross, Grant, *"Security Experts Question DOD Cybersecurity"*, 25 Jul 03, http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gen&story.id=41716 (accessed 2 Dec 06)

Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems, May 2005

Institute for Alternative Futures, "The Future Belongs to Those Who…A Guide for Thinking about the Future", www.altfutures.com

Joint Publication 1-02, 12 Apr 2001, as amended through 8 Aug 2006

Joint Publication 2-01.3, 24 May 2000, II-35

Kenyon, Henry S., *"Task Force Explores New Military Frontier"*, *Signal*, 11 Sep 06, http://imakenews.com/signal/e_article000653526.cfm?x=b11,0,w (accessed 1 Oct 06)

Kurzweil, Ray, *"The Singularity is Near"*, The Penguin Group, 2005

Lemos, Robert, *"Targeted Trojan Attacks on the Rise"*, dated 13 Oct 06, http://www.securityfocus.com/print/news/11418 (accessed 22 Nov 06)

Liang, Col Qiao and Col Wang Xiangsui, *Unrestricted Warfare*, Pan American Publishing Company, Panama City, Panama, 2002

Lopez, Kathleen A.K., Air Force News Statement, 19 Dec 05, http://www.aetc.af.mil/news/story_print.asp?storyID=123025914 (accessed 3 Dec 06)

Mullen, M. G., ADM USN, 16 Oct 06 Memorandum to Director, Strategic Studies Group, Subject: Strategic Studies Group XXVI Theme – "Fighting in Cyberspace in 2030", 16 Oct 06

National Science and Technology Council, *"Federal Plan for Cyber Security and Information Assurance Research and Development"*, April 2006. A copy can be accessed at http://www.nitrd.gov/

The National Strategy to Secure Cyberspace, Feb 2003

Onley, Dawn S. and Patience Wait, "*DOD's Efforts to Stave Off Nation-State Cyberattacks begin with China*", *Government Computer News*, 21 Aug 06,

Pew Internet & American Life Project, "*The Future of the Internet II*", 24 Sep 06, available at www.pewinternet.org

Roberts, Paul, "*DOD Cyber Sleuths Swap Secrets in Florida*", 12 Jan 05, http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/05/01/12/HNd (accessed 1 Oct 06)

Ryan Naraine, "*Microsoft: Trojans, Bots are Significant and Tangible Threat*", 12 June 06, http://www.eweek.com/article2/0,1759,1974620,00.asp (assessed 5 Dec 06)

SANS Top 20 Internet Security Attack Targets (2006 Annual Update), http://www.sans.org/top20/ (assessed 1 Oct 06)

Wynn, Michael W., "*Cyberspace as a Domain in which the Air Force Flies and Fights*", Air Force Link, 2 Nov 06, http://www.af.mil/library/speeches/speech.asp?id=283

Wynne, Honorable Michael W., Secretary of the Air Force, "*Letter to Airmen*", 3 November 2005, http://www.af.mil.library/viewpoints/secaf.asp?id=191 (accessed 29 Sep 06)

Wynne, Michael W. and Gen T. Michael Moseley, "*SECAF/CSAF Letter to Airmen: Mission Statement*", 7 Dec 05, http://www.af.mil.library/viewpoints/jvp.asp?id=192 (accessed 29 Sep 06)

End Notes

[1] Wynne, the Honorable Michael W., Secretary of the Air Force, *"Letter to Airmen"*, 3 November 2005, http://www.af.mil.library/viewpoints /secaf.asp?id=191 (accessed September 29, 2006)
[2] Air Force News Statement, December 9, 2005, , http://af.mil/pressreleases/story_print.asp?storyID=123013463 (accessed September 29, 2006)
[3] Ibid.
[4] Wynne, Michael W. and Moseley, General Michael T., *"SECAF/CSAF Letter to Airmen: Mission Statement"*, December 7, 2005 http://www.af.mil.library/viewpoints/ jvp.asp?id=192 (accessed September 29, 2006)
[5] For more information, see: Gibson, William, *Burning Chrome*, Eos Publishers, New York, NY, 2003 Edition, 224 pages and William Gibson, *Neruomancer*, 20th Edition, Ace Publishers, New York, NY, 2004, 384 pp. In the latter book, Gibson defined cyberspace as: "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts."
[6] Bush, President George W., *The National Strategy to Secure Cyberspace*, Office of the White House, Washington D.C., February 2003, 76 pp.
[7] Meyers, General Richard B., *The National Military Strategy for the United State: A Strategy for Today: A Vision for Tomorrow*, Office of the Chairman of the Joint Chiefs of Staff, Washington, D.C., 2004, 38 pp.
[8] Dr. Lani Kass is Special Assistant to the Chief of Staff, U.S. Air Force, and Director of the CSAF's Cyberspace Task Force, Washington, D.C. Established in January 2006, the Cyberspace Task Force's mission is to investigate cyberspace as a domain in and through which the Air Force flies and fights, to deliver sovereign options for the defense of the United States of America and its global interests. For more information, see her official biography at http://www.af.mil/bios/bio.asp?bioID=8507
[9]Air Force News Statement, 6 Apr 06, http://www.af.mil/news/story.asp?id=123018708 (accessed November 22, 2006)
[10] Henry S. Kenyon, *"Task Force Explores New Military Frontier"*, *Signal*, September 11, 2006, http://imakenews.com/signal/e_article000653526.cfm?x=b11,0,w (accessed October 1, 2006)
[11] "Security Experts Question DOD Cybersecurity", *InfoSec News*, July 25, 2003, http://landfield.com/isn/mail-archive/2003/Jul/0120.html (accessed September 29, 2006)
[12] Clark, Richard A., Testimony to the Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, April 8, 2003, p. 1
[13] Richard A. Clark is a former member of the Senior Executive Service, specialized in intelligence, cyber security and counterterrorism. He served as advisor to four presidents: Ronald Reagan, George H.W. Bush, William Clinton, and George W. Bush, where he served as the chief counter-terrorism to the National Security Council. He resigned from government service in Jan 2003.
[14] Clark, 2
[15] The SANS Institute (SysAdmin, Audit, Networking, and Security) is a trade name owned by the for-profit Escal Institute of Advanced Technologies. SANS provides computer security training, professional certification, and a research archive. It was founded in 1989. Additional information may be found on their website at: http://www.sans.org as of November 19, 2007
[16] SANS Top 20 Internet Security Attack Targets (2006 Annual Update), http://www.sans.org/top20/ (assessed November 19, 2007)
[17] Microsoft Corporation is a multinational computer technology corporation with global annual revenue of $44.28 billion and 71,553 employees in 102 countries as of July 2006.

Microsoft Corporation is one of the world's largest software companies. It develops, manufactures, licenses, and supports a wide range of software products for computing devices. Headquartered in Redmond, Washington, USA, its best selling products are the Microsoft Windows operating system and the Microsoft Office suite of productivity software, each of which has achieved near-ubiquity in the desktop computer market. Additional information is available at http://www.microsoft.com/en/us/default.aspx as of November 19, 2007

[18] A bot is a type of Trojan that communicates through an Inter Relay Chat (IRC) networks. Internet bots, also known as web robots, are automated internet applications controlled by software agents. These bots interact with network services intended for people, carrying out monotonous tasks and behaving in a humanlike manner. Bots can gather information, reply to queries, provide entertainment, and serve commercial purposes. More malicious use of bots is the coordination and operation of an automated attack on networked computers, such as a denial-of-service attack.

[19] A rootkit is a set of software tools intended to conceal running processes, files or system data from the operating system. Rootkits have their origin in relatively benign applications, but in recent years have been used increasingly by malware, helping an intruder to maintain access to a system whilst avoiding detection. Rootkits are known to exist for a variety of operating systems such as Linux, Solaris and versions of Microsoft Windows. Rootkits often modify parts of the operating system or install themselves as drivers or kernel modules.

[20] Malware or Malicious Software is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a portmanteau of the words "malicious" and "software."

[21] In the context of computer software, a Trojan horse is a malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse.

[22] Ryan Naraine, "*Microsoft: Trojans, Bots are Significant and Tangible Threat*," June 12, 2006 http://www.eweek.com/article2/0,1759,1974620,00.asp (assessed December 5, 2006)

[23] SecurityFocus claims it is the most comprehensive and trusted source of security information on the Internet. SecurityFocus is a vendor-neutral site that provides objective, timely and comprehensive security information to all members of the security community, from end users, security hobbyists and network administrators to security consultants, IT Managers, CIOs and CSOs. The organization reports over 18 million page views a month and 2.5 million unique users annually. Its website is http://www.securityfocus.com

[24] Robert Lemos, "Targeted Trojan Attacks on the Rise", dated October 13, 2006, http://www.securityfocus.com/print/news/11418 (accessed November 22, 2006)

[25] Ibid.

[26] Ibid.

[27] United States Computer Emergency Readiness Team Website, http://www.us-cert.gov/aboutus.html (accessed January 13, 2007)

[28] United States Computer Emergency Readiness Team, "Quarterly Trends and Analysis Report," dated November 28, 2006, http://www.us-cert.gov/press_room/trendsandanalysisQ406.pdf (accessed January 13, 2007)

[29] *"US Air Force Selects McAfee to Combat Spyware"*, August 17, 2006, http://www.spywarehunter.org/entry/us-air-force-selects-mcafee-to-combat-spyware/ (assessed February 18, 2007).

[30] The CERT/CC was created by DARPA in November 1988 after the Morris worm struck. It is a major coordination center in dealing with internet security problems. CERT is a center of internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. CERT studies internet security vulnerabilities, research long-term changes in networked systems, and develop information and training to help improve security. Additional information can be found at http://www.cert.org

[31] As of the original draft date of this paper, 2006 was set to beat that record, having already recorded 5,340 vulnerability reports through the 3rd Quarter of 2006 (Data from CERT/CC Statistics) See: http://www.cert.org/stats/cert_stats.html as of December 1, 2006.
[32] Ibid.
[33] Ibid.
[34] Liang, Colonel Qiao and Ziangsui, Colonael Want, *Unrestricted Warfare*, (Pan American Publishing Company, Panama City, Panama, 2002), p. 4
[35] Ibid. pp. 111-112.
[36] Onley, Dawn S. and Wait, Patience, *"DOD's Efforts to Stave Off Nation-State Cyberattacks begin with China"*, *Government Computer News*, August 21, 2006, http://www.gcn.com/cgi-bin/udt/im.display.printable?client.id=gen&story.id=41716 (accessed December 2, 2006)
[37] Ibid.
[38] CRS Report to Congress, "*Cyberwarfare*", June 19, 2001, p. 12
[39] China View, *"Chinese Army Holds "Vanguard-206B" Drill in E. China*," November 19, 2006, http://news.xinhuanet.com/english/2006-11/19/content_5349105.htm (accessed January 20, 2007)
[40] John Arquilla, PBS Interview, March 4, 2003, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html (accessed January 20, 2007)
[41] Serbian, John A. Jr., CIA Information Operations Issue Manager, *Statement for the Record before the Joint Economic Committee on Cyber Threats and the US Economy*, February 23, 2000 https://www.cia.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html (accessed January 20, 2007)
[42] Billo, Charles and Chang, Welton , *Cyber Warfare, An Analysis of the Means and Motivations of Selected Nation States*, December 2004 http://www.ists.dartmouth.edu/directors-office/execsum.pdf (accessed January 20, 2007)
[43] Hershman, Tania, "Israel Discusses the Inter-Fada", *Wired News*, January 12, 2001, http://www.wired.com/news/politics/0,1283,41154,00.html (accessed 19 Jan 07)
[44] Westerman, Toby, "Cyber Attack Aimed at U.S.?", *International News Analysis*, June 21, 2006 http://www.traditioninaction.org/HotTopics/i46htWesterman_Cyberattack.html (accessed January 19, 2007)
[45] Hal Fair quote, http://www.quotatio.com/f/ (accessed December 2, 2006)
[46] GAO Report, *Computer Security Hackers Penetrate DOD Computer Systems (GAO/T-IMTEC-92-5)*, 20 Nov 91, accessed through Global Security.org website, http://www.globalsecurity.org/security/library/report/gao/145327.pdf
[47] US Senate Permanent Subcommittee on Investigations, *"Security in Cyberspace"*, June 5, 1996, http://www.fas.org/irp/congress/1996_hr/s9606052.htm (accessed January 14, 2007)
[48] *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998 http://www.cybercrime.gov/white_pr.htm (accessed January 13, 2007)
[49] *"National Security Strategy to Secure Cyberspace"*, February 2003, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (accessed January 13, 2007)
[50] Ibid, viii.
[51] Gertz, Bill, "Chinese Hackers Prompt Navy College Site Closure", *The Washington Times*, November 30, 2006, http://www.washtimes.com/national/20061130-103049-5042r.htm (accessed February 18, 2007)
[52] Josh Rogin, "Network Attack Disables Naval War College", *FCW.com News*, November 30, 2006, http://www.fcw.com/article96957-11-30-06-Web (accessed February 18, 2007).
[53] Ibid.
[54] Air Force News Statement, December 9, 2005, http://af.mil/news/story_print.asp?storyID=123026382

[55] Air Force News Statement, December 9, 2005, http://af.mil/news/story.asp?storyID=123026382. (accessed 29 Sep 06)
[56] CRS Report to Congress, *"Creating a National Framework for Cybersecurity: An Analysis of Issues and Options"*, February 22, 2005, p. 7
[57] Microsoft Research Asia, http://research.microsoft.com/aboutmsr/labs/asia/default.aspx (accessed February 18, 2007).
[58] Ibid.
[59] A backdoor is a *"mechanism surreptitiously introduced into a computer system to facilitate unauthorized access to the system"* and can be classified into (at least) three categories: **Active.** Active backdoors originate outbound connections to one or more hosts. These connections can either provide full, fluid network access between the hosts (i.e. reverse tunnel-based) or be part of a process that actively monitors the compromised system, records information, sends data out in distinct "chunks" and receives both acknowledgements and/or commands from the remote systems. **Passive.** Passive backdoors listen on one or more ports for incoming connections from one or more hosts. Similar to the active backdoors, these programs can either be used to establish a forward tunnel into the compromised network or accept distinct commands and return the requested information. **Attack-based.** This category of backdoor could also be classified as the "unknown backdoor." It generally arises from a buffer-overflow exploit of poorly-written programs resulting in some type (e.g. root/Administrator-level, user-level, fully-interactive, one-instruction) of command-level access to the compromised system. There is one common element among the three types of backdoors - they all work by *circumventing the elaborate multi-layer security infrastructure* you have worked diligently to design and deploy. Most real (i.e. non-script-kiddies) hackers can determine almost immediately if it's worth attempting to meet your perimeter routers and firewalls with a head-on attack. Additional information can be found at http://www.securityfocus.com/infocus/1701 (accessed January 15, 2007).
[60] "Consensus Minimum Security Benchmarks", Fall 2002 Newsletter, http://iac.dtic.mil/iatac (accessed September 29, 2006)
[61] Joint Publication 2-01.3, 24 May 2000, II-35
[62] Gross, Grant, *"Security Experts Question DOD Cybersecurity"*, July 25, 2003 http://www.landfield.com /isn/mail-archive/2003/Jul/0120.html (accessed September 29, 2006)
[63] Ibid.
[64] Roberts, Paul, *"DOD Cyber Sleuths Swap Secrets in Florida"*, January 12, 2005 http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/05/01/12/HNd (accessed October 1, 2006)
[65] DISA Mission Statement, http://disa.mil/main/about/missman.html (accessed November 30, 2006)
[66] USSTRATCOM JTF-GNO Mission Statement, http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html (accessed November 30, 2006)
[67] DISA Information Assurance/NetOps Program Executive Office Mission Statement, http://disa.mil/peo-ian/index.html (accessed December 1, 2006)
[68] Wynne, Michael W. Wynn, "Cyberspace as a Domain in which the Air Force Flies and Fights,"Air Force Link, November 2, 2006, http://www.af.mil/library/speeches/speech.asp?id=283
[69] Navy Network Warfare Command Mission, http://www.globalsecurity.org/military/agency/navy/nnoc.htm (accessed October 2, 2006)
[70] 56th Communications Squadron, Air Force News Statement, June 16, 2006, http://www.luke.af.mil/news/story_print.asp?storyID=123031316 (accessed December 3, 2006)
[71] Lopez, Kathleen A.K., Air Force News Statement, December 19, 2005, http://www.aetc.af.mil/news/story_print.asp?storyID=123025914 (accessed December 3, 2006)

[72] Air Force Research Laboratory Mission Statement, http://www.afrl.af.mil/vision.asp (accessed December 1, 2006)
[73] Air Force Research Laboratory, Cyber Operations Branch Mission Statement, http://www.rl.af.mil/mission/missions.html#IFGB (accessed December 1, 2006)
[74] Visit to AFRL, August 30, 2006
[75] Briefing by Mr. Richard A. Raines during visit to AFRL, August 30, 2006
[76] Briefing by Mr. Richard A. Raines during visit to AFRL, August 30, 2006
[77] Marburger, John H. III and Kyamme, E. Floyd, "*Sustaining the Nation's Innovation Ecosystems, Information Technology Manufacturing and Competitiveness*", January 30, 2004 http://www.ostp.gov/PCAST/FINALPCASTITManuf%20ReportPackage.pdf (accessed January 19, 2007).
[78] Institute for Alternative Futures, "The Future Belongs to Those Who…A Guide for Thinking about the Future", www.altfutures.com
[79] National Science and Technology Council, "*Federal Plan for Cyber Security and Information Assurance Research and Development*, April 2006. A copy can be accessed at http://www.nitrd.gov/
[80] Briefing by Maj David L. Bibighaus (PhD) and Dr. Kamal Jabbour, visit to AFRL Rome Lab, September 12, 2006.
[81] Ibid.
[82] Ibid.
[83] Cybercraft Graphic, Permission for use by Maj David L. Bibighaus (PhD) and Dr. Kamal Jabbour, visit to AFRL Rome Lab, September 12, 2006
[84] Briefing by Maj David L. Bibighaus (PhD) and Dr. Kamal Jabbour, visit to AFRL Rome Lab, September 12, 2006
[85] SAS.Com, http://www.sas.com/success/ncdoc.html (accessed 18 Feb 07).
[86] Mullen, Admiral M. G., October 16, 2006 Memorandum to Director, Strategic Studies Group, Subject: Strategic Studies Group XXVI Theme – "Fighting in Cyberspace in 2030." "Cyberspace opens a new dimension to warfare. As we look to the future and try to predict where we will be engaged in warfare, consider warfare in the information age – not only is it a seamless blend of sensors, networks, and advanced information technologies, it is also different in principles and concepts."
[87] Ibid.
[88] Ibid.
[89] **QU**antum **BIT**. A data bit in quantum computing. Such an entity can hold more than two values. http://www.pcmag.com/encyclopedia_term/0,2542,t=qubit&i=50063,00.asp (accessed January 19, 2007)
[90] Quadrennial Defense Review Report, February 6, 2006, p. A-4
[91] National Science Board, *Science and Engineering Indicators, 2006*, http://www.nsf.gov/statistics/seind06/pdf/overview.pdf (accessed January 18, 2007)
[92] Ibid, p. 16.
[93] Ibid, p. 17.
[94] Ibid, p. 17.
[95] DISA Information Assurance/NetOps Program Executive Office Mission Statement, http://disa.mil/peo-ian/index.html (accessed December 1, 2006)
[96] Institute for Alternative Futures, *"The Future Belongs to Those Who…A Guide for Thinking about the Future"*, www.altfutures.com , p.2
[97] Kurzweil, Ray *"The Singularity is Near,"* (The Penguin Group, 2005), p 335

Center for Strategy and Technology

The Center for Strategy and Technology was established at the Air War College in 1996. Its purpose is to engage in long-term strategic thinking about technology and its implications for U.S. national security.

The Center focuses on education, research, and publications that support the integration of technology into national strategy and policy. Its charter is to support faculty and student research, publish research through books, articles, and occasional papers, fund a regular program of guest speakers, host conferences and symposia on these issues, and engage in collaborative research with U.S. and international academic institutions. As an outside funded activity, the Center enjoys the support of institutions in the strategic, scientific, and technological worlds.

An essential part of this program is to establish relationships with organizations in the Air Force as well as other Department of Defense agencies, and identify potential topics for research projects. Research conducted under the auspices of the Center is published as Occasional Papers and disseminated to senior military and political officials, think tanks, educational institutions, and other interested parties. Through these publications, the Center hopes to promote the integration of technology and strategy in support of U.S. national security objectives.

For further information on the Center for Strategy and Technology, please contact:

John P. Geis II, Col, PhD., Director
Theodore Hailes, Deputy Director

Air War College
325 Chennault Circle
Maxwell Air Force Base, Alabama 36112
(334) 953-5579/2985
(DSN 493-5579/2985)

Email: john.geis@maxwell.af.mil
ted.hailes@maxwell.af.mil

TITLES IN THE OCCASIONAL PAPERS SERIES

1
Reachback Operations for Air Campaign Planning and Execution
Scott M. Britten, September 1997

2
Lasers in Space: Technological Options for Enhancing U.S. Military Capabilities
Mark E. Rogers, November 1997

3
Non-Lethal Technologies: Implications for Military Strategy
Joseph Siniscalchi, March 1998

4
Perils of Reasoning by Historical Analogy: Munich, Vietnam, and the American Use of Force Since 1945
Jeffrey Record, March 1998

5
Lasers and Missile Defense: New Concepts for Space-Based and Ground-Based Laser Weapons
William H. Possel, July 1998

6
Weaponization of Space: Understanding Strategic and Technological Inevitables
Thomas D. Bell, January 1999

7
Legal Constraints or Information Warfare
Mark Russell Shulmann, March 1999

8
Serbia and Vietnam: A Preliminary Comparison of U.S. Decisions to Use Force
Jeffrey Record, May 1999

9
Airborne and Space-Based Lasers: An Analysis of Technological and Operational Compatibility
Kenneth W. Barker, June 1999

10
Directed Energy and Fleet Defense: Implications for Naval Warfare
William J. McCarthy, February 2000

11
High Power Microwaves: Strategic and Operational Implications for Warfare
Eileen M. Walling, March 2000

12
Reusable Launch Vehicles and Space Operations
John E. Ward, Jr., March 2000

13
Cruise Missiles and Modern War: Strategic and Technological Implications
David J. Nicholls, March 2000

14
Deeply Buried Facilities: Implications for Military Operations
Eric M. Sepp, March 2000

15
Technology and Command: Implications for Military Operations in the Twenty-First Century
William B. McClure, July 2000

16
Unmanned Aerial Vehicles: Implications for Military Operations
David Glade, July 2000

17
Computer Networks and Information Warfare: Implications for Military Operations
David J. Gruber, July 2000

18
Failed States and Casualty Phobia: Implications for Force Structure and Technology Choices
Jeffrey Record, December 2000

19
War as We Knew It: The Real Revolution in Military Affairs/Understanding Paralysis in Military Operations
Jan S. Breemer, December 2000

20
Using Lasers in Space: Laser Orbital Debris Removal and Asteroid Deflection
Jonathan W. Campbell, December 2000

21
Weapons for Strategic Effect: How Important is Technology?
Collin S. Gray, January 2001

22
U.S. Army Apache Helicopters and U.S. Air Force Expeditionary Forces: Implications for Future Military Operations
Brad Mason, June 2001

23
The End of Secrecy? Military Competitiveness in the Age of Transparency
Beth M. Kaspar, August 2001

24
Prompt Global Strike Through Space: What Military Value?
Larry G. Sills, August 2001

25
Precision Engagement at the Strategic Level of War: Guiding Promise or Wishful Thinking?
Timothy J. Sakulich, December 2001

26
Infrared Systems for Tactical Aviation: An Evolution in Military Affairs?
George B. Hept, January 2002

27
Unmanned Undersea Vehicles and Guided Missile Submarines: Technological and Operational Synergies
Edward A. Johnson, Jr., February 2002

28
Attack Operations For Missile Defense
Merrick E. Krause, May 2002

29
Death by a Thousand Cuts: Micro-Air Vehicles in the Service of Air Force Missions
Arthur F. Huber II, June 2002

30
Sustained Space Superiority: A National Strategy for the United States
Larry J. Schaefer, August 2002

31
Hyperspectral Imaging: Warfighting Through a Different Set of Eyes
Paul J. Pabich, October 2002

32
Directed Energy Weapons on the Battlefield: A New Vision for 2025
John P. Geis II, April 2003

33
Homeland Security and the Coast Guard: Postured for Technology Inprovements
Arthur C. Walsh, June 2003

34
Non-Lethal Weapons: Setting our Phasers on Stun? Potential Strategic Blessings and Curses of Non-Lethal Weapons on the Battlefield
Erik L. Nutley, August 2003

35
Aircrew Performance Cutting Edge Tech
Kris M. Belland, September 2003

36
Centralized Control with Decentralized Execution: Never Divide the Fleet
Daniel F. Baltrusaitus, May 2004

37
The Decision Maker's Guide to Robust, Reliable and Inexpensive Access to Space
Gary N. Henry, July 2004

38
Global Mobility: Anywhere, Anytime, Any Threat? Countering the MANPADS Challenge
Jacqueline D. van Ovost, July 2005

39
Strategies For Defeating Commercial Imagery Systems
Stephen Latchford, July 2005

57-59
Streamlining DOD Acquisition: Balancing Schedule With Complexity
Edited by Lt Col James Rothenflue and Marsha J. Kwolek

A System as the Enemy: A Doctrinal Approach to Defense Force Modernization
Benjamin A. Drew

Impact of Weapons Systems Complexity on Systems Acquisition
Robert A. Dietrick

Faster is Better...Can the USAF Acquisition Process be SAIV'D?
James L. Chittenden

60
The Seductive Effects of an Expeditionary Mindset
Michael Arnold

61
The Air Force in SILIC0 – Computational Biology in 2025
Christopher Coates, December 2007

62
Biofuels: An Alternative to U.S. Air Force Petroleum Dependency
Mark S. Danigole